

REMARKS

Claims 1-20 are pending in this application. Claims 1-20 are rejected. Claims 1, 4, 6, 8, and 17-19 are amended. Claims 7 and 17 are amended to clarify that the multiple daemons manage the remote nodes. Claim 12 is amended to correct an antecedent basis problem. No range of equivalents is surrendered or is intended to be surrendered by these amendments. Reconsideration and withdrawal of the rejections set forth in the last Office Action, as they may apply to the claims as set forth, is respectfully requested in view of the remarks set forth herein.

The specification is objected to because it contains an embedded hyperlink at p. 5, lines 24-27. The specification is amended above to delete the objected to hyperlink. Withdrawal of the objection is respectfully requested.

A copy of the current version of the publication reference that the objected to hyperlink referenced is also submitted herewith. Unfortunately, the version referenced in the hyperlink is no longer available.

Claims 1-9, 11-13, 15-17, and 19-20 are rejected under 35 U.S.C. § 103(A) as being rendered obvious by U.S. Patent No. 6,366,954 to Traversat et al. ("Traversat"). Applicants respectfully traverse this rejection. "To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art." MPEP 2143.03 (emphasis added). Traversat fails to teach or suggest all the claim limitations.

For example, Traversat does not teach or suggest "retrieving a list of persistent attributes from the object, wherein the persistent attributes are a subset of the attributes and wherein the persistent attributes each comprise a persistent attribute value," as recited in claims 1, 15, and 19. The cited col. 4, lines 25-37, col. 12, and col. 6, lines 19-28 do not teach or suggest this claimed feature. Claims 1, 15, and 19 are all directed at mapping objects onto a LDAP repository. Despite this, the cited sections in cols. 4 and 12 describe searching a portion of a *LDAP* server for one or more attributes (emphasis added) and the cited section in col. 6 only talks about the general capabilities of an *LDAP* software system (emphasis added). None of these sections, or elsewhere in Traversat, teach or suggest retrieving a list of attributes from an object that is to be mapped onto an LDAP repository, let alone a list of persistent attributes. Consequently, at least for these reasons claims 1, 15, and 19 are not rendered obvious by Traversat. Moreover, dependent claims 2-10, 16-18 and 20 are not rendered obvious by Traversat for at least these same reasons and the independent features that they recite. Allowance of these claims is respectfully requested.

Likewise, Traversat does not teach or suggest “determining a path, wherein the path identifies a location in the LDAP repository,” as recited in claims 1, 15, and 19. The cited column 6, lines 13-18 only discusses general LDAP naming conventions. It is implicit that the claimed method is determining a path in the LDAP repository that is new for the *to be* mapped object (since the object is being mapped, the path does not exist until determined by the determining step). Traversat does not teach or suggest this feature. Consequently, at least for this reason, claims 1, 15, and 19 are not rendered obvious by Traversat. Moreover, dependent claims 2-10, 16-18 and 20 are not rendered obvious by Traversat for at least this same reason and the independent features that they recite. Allowance of these claims is respectfully requested.

Regarding claim 11, Applicants respectfully note that claim 11 is not the method claim of claim 1, as stated on page 6 of the Office Action. Applicants respectfully request that the Examiner provided a detailed rejection of this claim or allow the claim. Furthermore, Traversat does not render obvious claim 11 at least because it does not teach or suggest “setting the persistent attributes in the object with the retrieved persistent attribute values.” Traversat is allegedly exchanging data between a java system database entry and an LDAP directory service. There is no teaching or suggestion in Traversat of setting the persistent attributes in an object with retrieved persistent attribute values. Consequently, at least for this reason, claim 11 is not rendered obvious by Traversat. Moreover, dependent claims 12-14 are not rendered obvious by Traversat for at least this reason and the independent features that they recite. Allowance of these claims is respectfully requested.

Applicants also specifically traverse any implication that the differences between Traversat and the claimed invention would have been obvious to one of ordinary skill in the art. The claimed invention and the absence of claimed features from Traversat speaks for itself. However, it is clear that the claimed invention is much more than “just an backward step using LDAP.” As noted in MPEP 2143.03, all the claim limitations must be taught or suggested by the prior art. The Office Action fails to do this.

Claims 10, 14, and 18 are rejected under 35 U.S.C. § 103(a) as being rendered obvious by Traversat in view of U.S. Patent No. 6,240,422 to Atkins et al. (“Atkins”). The combination of Traversat and Atkins does not teach or suggest each and every element of independent claims 1, 11, and 15. Specifically, the combination with Atkins does not overcome the deficiencies of Traversat described above. Moreover, Atkins does not teach or suggest the claimed features of claims 10, 14 and 18. For example, Atkins does not teach or suggest “wherein Java reflection is used to implement the setting step,” as recited in

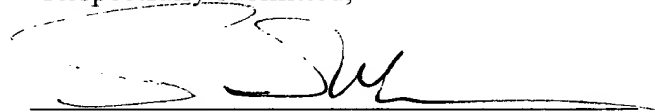
claim 14. Atkins does not teach or suggest the "setting" from claim 11. Consequently, claims 10, 14, and 18 are not rendered obvious by Traversat and Atkins. Allowance of these claims is respectfully requested.

CONCLUSION

In view of the above amendments and remarks, Applicants believe that all of the objections and rejections against this application have been fully addressed and that the application is now in condition for allowance. Therefore, withdrawal of the outstanding objections and rejections and a notice of allowance for the application is respectfully requested.

If the Examiner believes that a personal or telephonic interview would be of value in expediting the prosecution of this application, the Examiner is hereby invited to telephone the undersigned counsel to arrange for such a conference.

Respectfully submitted,



Date: September 7, 2004

Sean Wooden
Reg. No. 43,997
ANDREWS & KURTH LLP
1701 Pennsylvania Avenue, N.W.
Suite 300
Washington, D.C. 20006
Telephone: (202) 662-2738
Fax: (202) 662-2739

Attachment: HP Servicecontrol Manager 3.0 User's Guide

HP Servicecontrol Manager 3.0 User's Guide

Edition 2.1



Manufacturing Part Number: 5187-4543

October 2003

United States

© Copyright 2002-2003 Hewlett-Packard Development Company L.P.

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty

A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY
3000 Hanover Street
Palo Alto, California 94304 U.S.A.

Use of this document and any supporting software media supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs, in their present form or with alterations, is expressly prohibited.

Copyright Notice

Copyright © 2002-2003 Hewlett-Packard Development Company L.P. All rights reserved. Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

Trademark Notices

Itanium® is registered trademark of Intel Corporation.

Java® and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. Hewlett-Packard is independent of Sun Microsystems.

Microsoft® is U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark in the United States and other countries, licensed exclusively through The Open Group.

Publication History

The manual publication date and part number indicate its current edition. The publication date will change when a new edition is released. The manual part number will change when extensive changes are made.

To ensure that you receive the new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

- *HP Servicecontrol Manager 3.0 User's Guide*, 5187-4543
October 2003, Edition 2.1
- *HP Servicecontrol Manager 3.0 User's Guide*, 5971-4738
June 2003, Edition 2
- *HP Servicecontrol Manager 3.0 User's Guide*, 5187-1882
December 2002, Edition 1

New editions of this manual will incorporate all material updated since the previous edition. For the latest version, see the HP Servicecontrol Manager documentation on the Web:

<http://docs.hp.com/>

Please use the following Web form to send us feedback:

<http://docs.hp.com/assistance/feedback.html>

About this Guide

This guide describes installing, upgrading and getting started with Servicecontrol Manager. It also provides a basic overview of the Servicecontrol Manager functionality and terminology. It assumes that you are an HP-UX or Linux system administrator and familiar with installing and administering software in these environments.

This guide applies to HP Servicecontrol Manager 3.0. If you need information for a previous version of Servicecontrol Manager, go to the Web:

<http://docs.hp.com>

Typographic Conventions

We use the following typographical conventions.

<i>mxtool</i> (4)	HP-UX or Linux manual page. <i>mxtool</i> is the name and <i>r</i> is the section. From the command line, you can enter “man <i>mxtool</i> ” or “man 4 <i>mxtool</i> ” to view the man page. See <i>man</i> (1).
<i>Book Title</i>	Title of a book. On the Web and on the Instant Information CD, it may be a hot link to the book itself.

Command	Command name or qualified command phrase.
ComputerOut	Text displayed by the computer.
<i>Emphasis</i>	Text that is emphasized.
Emphasis	Text that is strongly emphasized.
KeyCap	Name of a keyboard key. Note that Return and Enter both refer to the same key.
Term	Defined use of an important word or phrase.
UserInput	Commands and other text that you type.
<i>Variable</i>	Name of a variable that you may replace in a command or function or information in a display that represents several possible values.
[]	Contents are optional in formats and command descriptions. If the contents are a list separated by , you must choose one of the items.
{ }	Contents are required in formats and command descriptions. If the contents are a list separated by , you must choose one of the items.
...	Preceding element may be repeated an arbitrary number of times.
	Separates items in a list of choices.

1. HP Servicecontrol Manager Introduction

HP Servicecontrol Manager Overview	8
The Management Domain	10
Nodes	10
Node Groups	10
Central Management Server	11
Network client	12
Users and Roles	13
Master Role	13
Trusted User	14
Tools	16
Tool Types	16
Management Protocols and Applications	16
Information Storage	18
SCM Audit Log	18
Database Repository	18
Security and Access	19
Secure Access	19
Secure Transactions	20
Increased Security Options	23

2. Installing HP Servicecontrol Manager

Installation Overview	26
System Requirements	28
Installing Servicecontrol Manager on HP-UX	30
Before You Install CMS Software on an HP-UX Server	30
Installing CMS Software on an HP-UX Server	31
Installing Servicecontrol Manager on Linux	33
Before You Install CMS Software on a Linux Server	33
Installing CMS Software on a Linux Server	34
Adding Managed Nodes	37
Upgrading from Servicecontrol Manager 2.5 to 3.0	41
Additional Suggested Removal and Clean-up Tasks	43
Manually Converting a Tool From SCM 2.5 to 3.0	43
Updating to Servicecontrol Manager 3.0 Version 3.00.04	45
Removing Servicecontrol Manager	46

3. Getting Started with SCM

Types of SCM Users	48
Getting Started Using SCM	49
Getting Started Administering SCM	52

4. Increasing Servicecontrol Manager Security

Replace Self-Signed Tomcat Certificates	56
Enable WBEM Certificate Validation	57
Encrypt Java RMI Transactions	60

Contents

Disable the Tomcat Web Server	61
Manage SCM Software	62
Inspect the Audit Log Regularly	62
Restrict root access on the CMS.	62
Change Generated Passwords	62
Closely Manage SCM Authorizations	62
Verify Security Dependencies	63
Software Security Dependency	63
Network Security Dependency.....	63
 Glossary	65
 Index	69

HP Servicecontrol Manager Introduction

This chapter introduces the basic concepts and functionality of the HP Servicecontrol Manager.

The following topics are covered in this chapter:

- “HP Servicecontrol Manager Overview” on page 8
- “The Management Domain” on page 10
 - “Nodes” on page 10
 - “Central Management Server” on page 11
- “Users and Roles” on page 13
 - “Master Role” on page 13
 - “Trusted User” on page 14
- “Tools” on page 16
 - “Tool Types” on page 16
 - “Management Protocols and Applications” on page 16
- “Information Storage” on page 18
 - “SCM Audit Log” on page 18
 - “Database Repository” on page 18
- “Security and Access” on page 19
 - “Secure Access” on page 19
 - “Secure Transactions” on page 20
 - “Increased Security Options” on page 23

HP Servicecontrol Manager Overview

SCM is an easy-to-use, multi-system management solution with a Web-enabled interface and a command line interface. SCM delivers multi-system access to all key system administration tools for fault monitoring, configuration, and workload management. Administrators with multiple HP systems running primarily HP-UX or Linux benefit the most from using SCM.

SCM provides management of more systems with increased control and decreased errors throughout the IT environment. The biggest advantage is SCM's synergistic integration of multiple administrative tasks providing a significant improvement in productivity for virtually all multi-system configurations. In fact, sites with multiple HP servers with similar or the same configurations experience as much as a 5x improvement in system administration productivity when they implement SCM. SCM provides system administrators with:

- *Increased productivity* through a single point of administration for HP-UX, Linux, and Windows manageability tools (Windows manageability provided through launching HP Proliant Insight Manager7)
- *Increased efficiency* through multi-system management capabilities such as group operations and role-based management
- *Improved security* through roles-based management, authentication and encryption
- *Ensured accountability* through audit logging of changes across the IT environment
- *Expanded flexibility* through the use of customized scripts and commands executed across multiple systems simultaneously

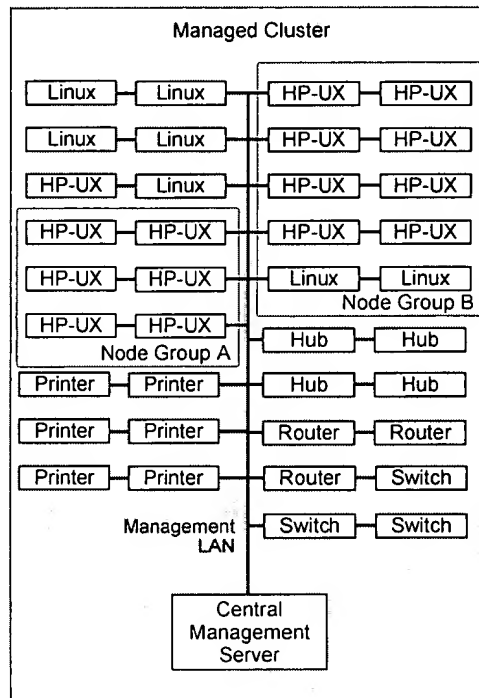
Features	Benefits
Choice of management interfaces – Web-enabled graphical user interface or command line interface	Provides options for remote management that span an intuitive graphical user interface to a command line interface for fast, low-bandwidth operations.
Group operations – simultaneously launch management tasks across multiple servers	Increases efficiencies, especially in environments with large server farms that have similar configurations.
Role-based management – assign administrators access to certain manageability tools for specific managed nodes or node groups	Reduces error-caused downtime by allowing the delegation of administrative tasks without a proliferation of root privileges.
Audit logging – log task information including: 1) the target nodes; 2) the result of the action; 3) the tool name used to perform task; 4) the user name who performed the task	Ensures accountability for actions and tracks changes across the IT environment.

Features	Benefits
Security – secure authentication between the managed node and the central management server (CMS), as well as between the CMS and the network client	Increases confidence knowing that the transactions between the network client, the CMS, and the managed nodes are all authenticated and encrypted.
Customized scripts and commands – easily customize frequently used scripts and commands	Provides the ability to add current scripts and commands into SCM and execute them across multiple systems simultaneously.
Access to HP-UX, Linux, and Windows management tools – launch HP-UX, Linux, and Windows (via user-defined launch of HP Insight Manager7) management tools from the SCM CMS	Provides a single point of control for HP-UX and Linux manageability tools. HP Insight Manager7, which can also be integrated into SCM, provides Windows monitoring and device management.

The Management Domain

The management domain is a collection of resources that are placed under the control of the SCM. The dark-shaded area in Figure 1-1 represents a management domain. The individual resources are called managed nodes. One node in each management domain is the central management server (CMS). For more information about the CMS, see “Central Management Server” on page 11.

Figure 1-1 Management Domain



Nodes

Resources that make up a management domain are called managed nodes. A node can be any device on the network that can communicate with SCM, which includes servers, printers, workstations, hubs, and routers. In most cases, these devices will have an IP address or a MAC address associated with them.

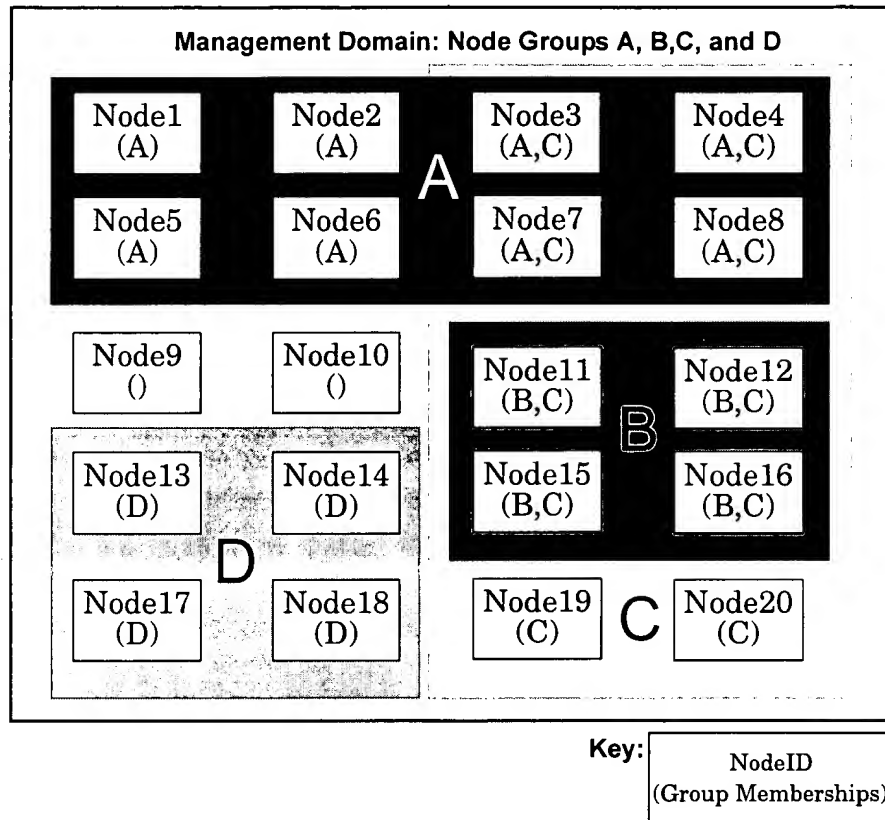
Each node can have a variety of management protocols or management applications installed. SCM tools use these protocols or applications to perform tasks, monitor software, and monitor hardware on the managed nodes.

Node Groups

Node groups are a powerful way to divide and organize your management domain into manageable units. Often the nodes that belong to a node group have something in common such as operating system, backup schedule, system function, or hardware type. Working with node groups increases your efficiency because you can perform a task on each node in a node group by performing a single task.

Nodes can belong to one or more node groups, but they do not have to belong to a node group. A node group cannot be a member of another node group, but all the nodes of a node group can be completely contained within another node group. In Figure 1-2, Node11 is in node groups B and C. Nodes 9 and 10 represent nodes that do not belong to a node group.

Figure 1-2 Node Groups in a Management Domain



Central Management Server

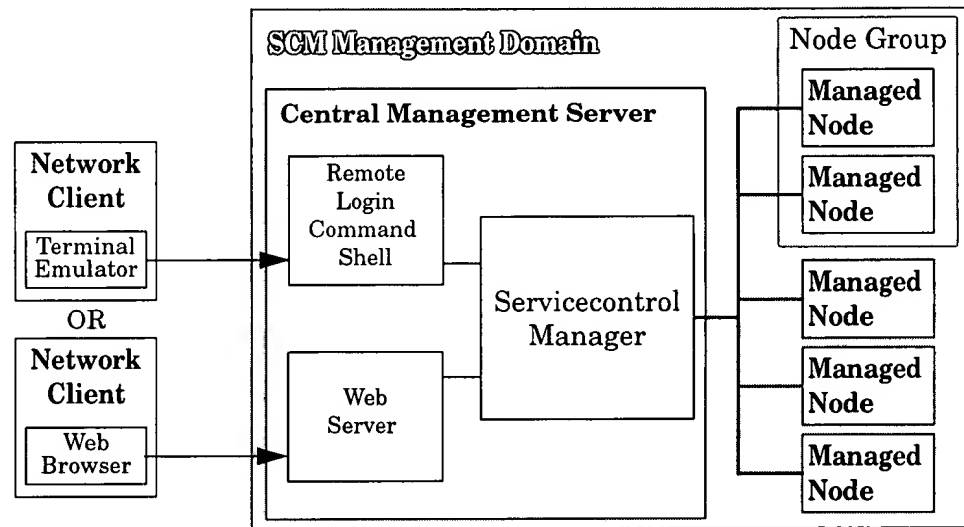
The central management server (CMS) is the node in the management domain that executes the SCM software and initiates all central operations within the SCM. In addition to the SCM software, the CMS maintains a data repository using MySQL relational database for storage of persistent objects. Typically, servers for the multiple-system aware applications, such as Software Distributor (SD) and Ignite-UX (IUX), also reside on the CMS. These applications are not required to reside on the CMS; they can reside anywhere on the network.

Since the CMS is a node within the management domain, it manages itself as part of the domain. You can add the CMS as a node within another management domain if you want to manage it using a separate CMS.

Network client

SCM can be accessed from *any* network client. The network client can be part of the management domain, but it doesn't have to be. Figure 1-3 represents the relationship between a network client, the CMS, and several managed nodes.

Figure 1-3 Network Client, CMS, and Managed Node Relationship

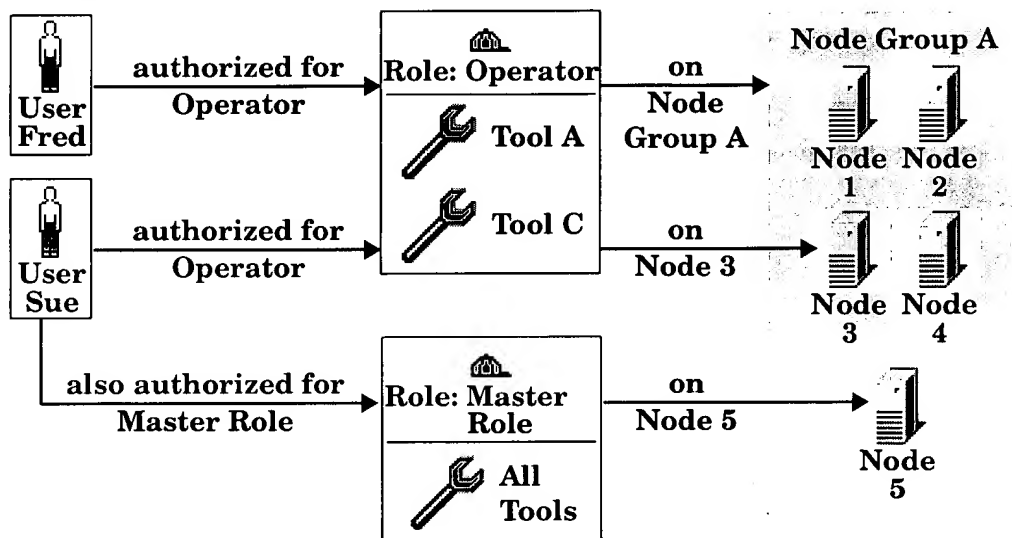


Users and Roles

An SCM user can be anyone with a valid operating system login on the CMS. Once a user is added to SCM, then he can be authorized for roles on one or more nodes in the management domain. Figure 1-4 represents the relationship between users, roles, and nodes or node groups.

Figure 1-4

Users and Roles



A role defines the responsibilities associated with an operation or process. Each role is associated with a set of SCM tools that a user might need for a particular task, such as database administration or software management. Authorizing a user for a role on a node or node group enables the user to run the associated set of tools on that node or node group. For example, the *web admin* role enables a user to access tools required for administering a Web server. In Figure 1-4, Fred is authorized for the *operator* role on *node group A*. He can use *tool A* or *tool C*, which are associated with the *operator* role, to manage all the nodes in *node group A*.

IMPORTANT

Role assignments enable non-root users to run tools as root or as another specified user. Be careful when granting non-root users permission to run tools as root. Take into consideration all the capabilities given by a tool, above and beyond the capabilities it is designed for, before you associate it with a role.

You can have up to 32 roles in SCM including the master role. The master role is the only default role installed with SCM.

Master Role

The master role provides complete access to all tools for the authorized node or node group. When a tool is added to SCM, the master role is automatically associated with the tool. Tools cannot be removed from the master role, and the master role cannot be

deleted from SCM. All other roles can be enabled, disabled, or deleted. If you don't want a user to have access to all available tools for a specific node or node group, they should not be authorized for the master role on that node or node group.

CAUTION

A user assigned the master role on the CMS can execute commands as any user. Therefore, this user could grant trusted user privilege to himself.

Trusted User

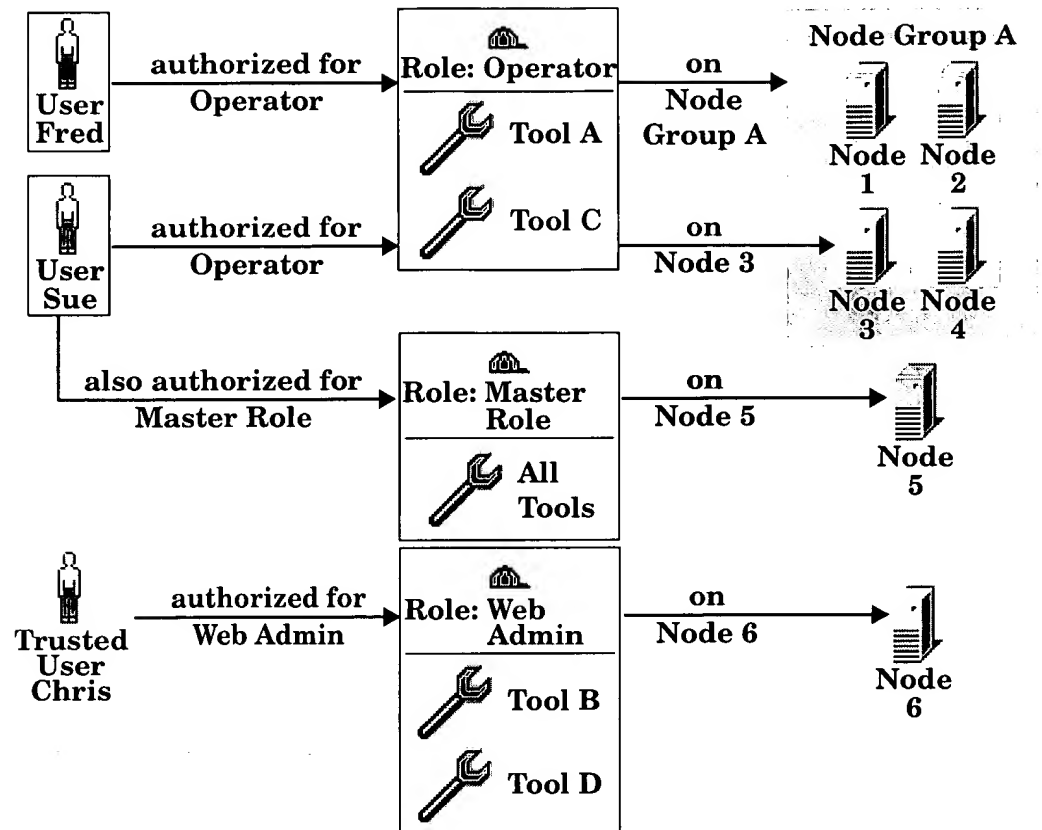
A trusted user is a user who has been given a special privilege to administer the SCM software. Trusted users manage:

- authorizations
- nodes
- node groups
- users
- roles
- tools

In addition, trusted users maintain and backup the repository and monitor the SCM audit log.

By default, root on the CMS is assigned the trusted user privilege, but this privilege can later be revoked. The trusted user privilege can be given to one or more users, and SCM requires that at least one user is a trusted user. A trusted user is not automatically authorized to execute tools. Trusted users must be authorized for roles on specific nodes or node groups just like any other user.

Figure 1-5 Users and Trusted Users



In Figure 1-5, the only difference between Chris, Sue, and Fred is that Chris manages the SCM software. He can authorize himself or any other user to perform a role on a node or node group. With the current authorizations, Chris is limited to using only tools B and D on node 6.

Tools

Tools are applications, commands, or scripts that are launched from within SCM. You can add custom tools into SCM and execute them across multiple systems simultaneously.

Tool Types

There are three types of tools supported in the SCM environment: Web tools, X Window tools, and command line tools.

Web tools	Web tools must reside on a Web server. The Web server can be running on the CMS or on a managed node. SCM launches the URL from a command line or from the graphical user interface. When a Web tool is launched from the command line, SCM opens a browser to display the tool. When a Web tool is launched from the SCM graphical user interface, it is opened in the workspace or in a separate browser window.
X Window tools	X Window tools require that an X server is running. These tools can reside on the CMS or on a managed node. When accessing SCM from a network client, you must have X server software running on the network client to execute an X Window tool. From the command line or the graphical user interface, SCM invokes the X Window application using the command line and passes the location of the X server by requesting the device for display from the user.
Command line tools	Command line tools include applications, commands, and scripts. They can reside on the CMS or on another managed node. They can be launched directly from the command line or from the graphical user interface.

Management Protocols and Applications

The basic supported management protocols and applications are Distributed Task Facility (DTF), WBEM, and SNMP. Tools are not limited to these protocols or applications, and they can even provide a custom management protocol or application. If a particular tool requires the DTF management application to be running, then the tool won't be able to run on a system where the DTF agent software isn't installed.

Distributed Task Facility

The distributed task facility (DTF) improves operator efficiency by replicating operations across the nodes or node groups within the management domain using a single command. This reduces the load on administrators in multi-system environments. X Window tools and command line tools use the DTF to execute. The DTF supports:

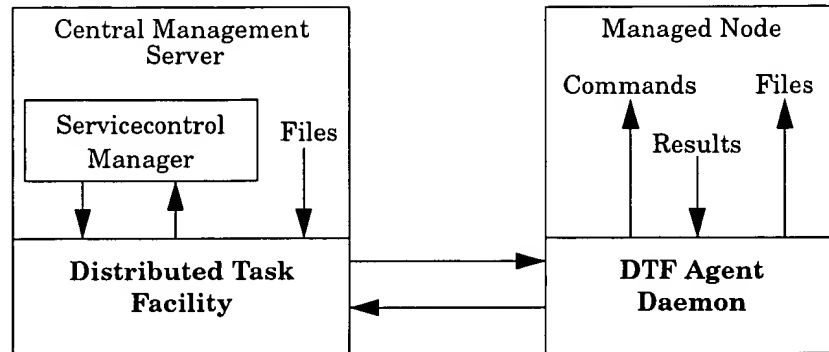
- Executing scripts, commands, and applications remotely on managed nodes

- Copying files to managed nodes

The DTF connects the CMS to agent software running on each node in the cluster. This is shown in Figure 1-6.

Figure 1-6

Distributed Task Facility



The DTF communicates to the agent daemon what tasks need to be performed on the node. The agent then performs the tasks and returns the results to the DTF. The DTF consolidates the feedback it receives from all the agents.

Information Storage

SCM uses an audit log and a database repository to track activity and store your management domain information.

SCM Audit Log

SCM logs all tasks performed by all SCM users on all nodes. The information is stored in the audit log on the CMS. Each managed node that has the DTF agent running also keeps a separate audit log that contains just the tasks performed on that node. The complete SCM audit log on the CMS and the audit log for the individual managed nodes are both located at: `/var/opt/mx/logs/mx.log`.

SCM logs all tasks with the following information:

- time stamp
- SCM user name
- nodes
- event
- tool result

By default, the `stdout` and `stderr` of command execution is logged (verbose level) for all nodes. Commands like `bdf` or `ls` frequently have large and time sensitive output. Therefore, the XML tool definition file provides options for logging or not logging the command output. In addition, other aspects of the audit log, such as maximum file size, can be configured in the `log.properties` file.

More information about configuring and maintaining the audit log is available in the SCM online help.

Database Repository

SCM uses a repository database to store vital management domain information. The repository contains information about:

- authorizations
- nodes
- node group definitions
- users
- passwords
- role definitions
- tool definitions

Database Software

SCM uses MySQL for the database. MySQL is an open source relational SQL database developed by MySQL AB. Information about MySQL and MySQL AB is available at <http://www.mysql.com>.

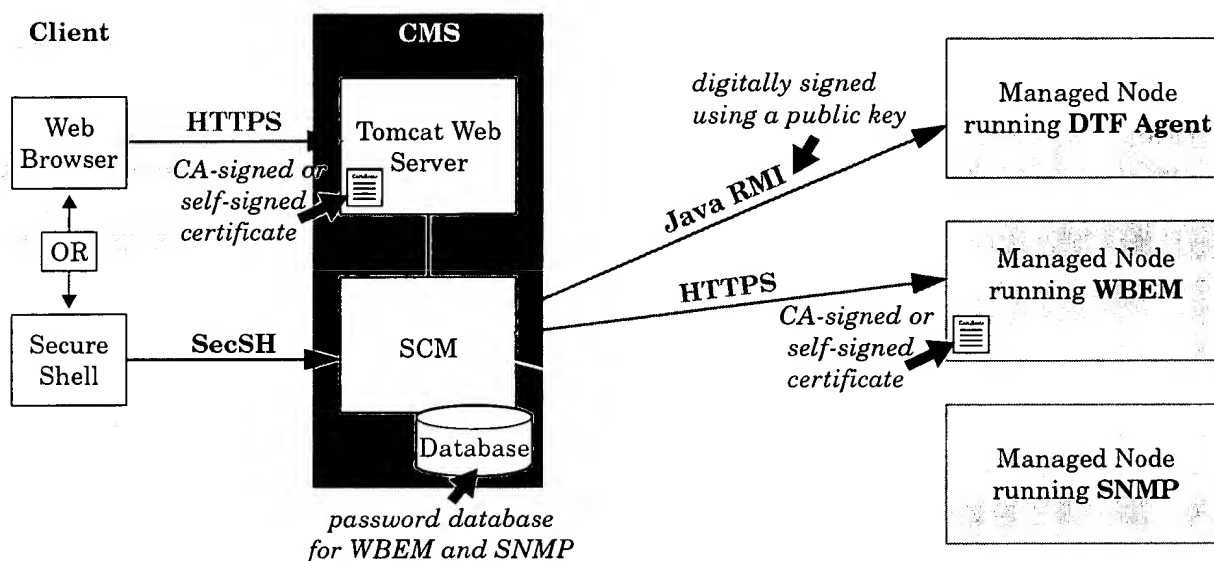
More information about backing up and restoring the SCM repository is available in the SCM online help.

Security and Access

SCM utilizes several technologies to provide secure access and secure transactions. The security model is graphically represented in Figure 1-7.

To simplify the image, each managed node in Figure 1-7 is only running one management application or protocol. Normally, managed nodes are running multiple management applications and protocols.

Figure 1-7 SCM Security



Secure Access

You can access SCM via a command line or a Web browser. Both of these user interfaces can be accessed from anywhere on your network.

When you access SCM from the command line interface, your operating system login automatically logs you on to SCM. Once you are logged on, you will have access to use the SCM commands based on your authorizations. If you access SCM from any system other than the CMS, make sure you use an Secure Shell (SecSH). Programs like telnet, rlogin, and ftp do not provide encrypted access. When you use one of these applications to access SCM, your data including your password is transmitted across the network unencrypted. In addition, these protocols are not spoof-protected.

When you access the SCM from a Web browser, you log on using the secure HTML log-on screen. The user name and password for the log-on screen are the same as your CMS operating system user name and password. Your information is securely transmitted using the SSL protocol. SSL provides data encryption and server authentication by using a public and private key technology. The Web server on the CMS uses a certificate for server authentication. By default, this certificate is self-signed, but it may be replaced by a certificate that is signed by a trusted certificate authority.

Secure Transactions

The security of the transaction depends on your networking environment and on the management application or protocol that each tool is using.

Java® Remote Method Invocation (RMI) Transactions

The distributed task facility uses Java RMI to communicate with the DTF agents. Transactions are digitally signed using the public keys, which provides authentication protection but not encryption. Passwords should not be transmitted to or from DTF tasks. For example, a DTF task command line should not contain a password and the task results should not contain a password.

For information about how to add encryption, see Chapter 4, “Increasing Servicecontrol Manager Security,” on page 55.

X Applications The data exchanged between an X client (or application) running on a managed node and an X server on the network client is transmitted in clear text over the network. X clients are not recommended in environments where security is a concern.

HTTPS Transactions

HTTPS provides secure communication for any tool or management application using the Web Based Enterprise Management (WBEM) protocol. WBEM is an industry standard that simplifies system management. It provides access to both software data and hardware data that is readable by WBEM compliant applications.

SCM keeps a database of passwords for managed nodes running WBEM. The database contains the user names and passwords for each managed node, which are required to provide user authentication for tools using this protocol. These accounts do not need to have other access capabilities, such as log on rights. They are only used for WBEM access by SCM. The WBEM username and password can be set from the command line or the graphical user interface. For more information, see *administering nodes - editing node security* or *administering node groups - editing node group security* in the SCM online help.

WBEM passwords for each user should be unique on each managed node for increased security. This will prevent someone from gaining access to a user account on all managed nodes.

Additional information about HP WBEM Services is available at:

<http://docs.hp.com/hpux/netsys/index.html>

Web Server Security SCM uses the Tomcat Web server on the CMS. Tomcat features that are not required by SCM are turned off by default. This includes Server Side Includes and Common Gateway Interface scripts.

Self-Signed Certificates The self-signed certificates used for WBEM and Tomcat Web server authentication make it possible for another system operating with the same IP address and hostname to impersonate the CMS. Use CA-signed certificates to prevent this possibility. If CA-signed certificates are not used, save the certificate in the browser the first time the browser is used to access SCM. This minimizes the chance of a possible “man-in-the-middle” attack on certificate authority.

For information about how to upgrade to CA-signed certificates, see Chapter 4, “Increasing Servicecontrol Manager Security,” on page 55.

SNMP Transactions

SNMP Versions 1 and 2 are not secure protocols. Therefore, anyone with access to your network will be able to intercept and view SNMP transactions. SCM does not use SNMP SetRequests. By default, the supported operating system platforms have SNMP SetRequests disabled. For improved security, do not enable SNMP SetRequests on the CMS or on the managed nodes. Even SNMP GetRequest responses can be spoofed, so all information from SNMP should be regarded as untrusted.

SCM keeps a database of read and write community names for managed nodes running SNMP. The community name must match those configured on the management node. The SNMP community names and passwords can be set from the command line or the graphical user interface. For more information, see *administering nodes - editing node security* or *administering node groups - editing node group security* in the SCM online help.

Managing Servers Behind a Firewall

SCM supports managing servers that are located behind a firewall when using the WBEM protocol. The firewall must be configured to allow the WBEM traffic through the firewall. This traffic uses HTTPS over TCP port 5989. SNMP and DTF communications are not recommended through a firewall because the data exchanged between the CMS and the managed nodes is not encrypted.

Ports Used

If your CMS or managed nodes are using a host-based firewall such as IPFilter, you will need to allow these new ports access through the firewall. The Bastille product on HP-UX can help with the IPFilter configuration.

The following information is provided to assist in using SCM in a secured environment. Its completeness has not been verified, so some experimentation may be needed to apply it. The outbound traffic on these sockets are only in response to inbound connections. See *reference - ports* in the SCM online help for information on configuring the ports that are configurable.

SCM uses the following fixed ports on the *CMS only*:

Service	Port	Protocol	Used By	Configurable?
HTTP	280 Inbound/Outbound	TCP	Apache Tomcat	No
HTTPS	50000 Inbound/Outbound	TCP	Apache Tomcat	Yes
HTTPS	50005 Local host only	TCP	Apache Tomcat	Yes
RMI	Anonymous (see section below) Inbound/Outbound	TCP	Apache, SCM Daemons	Yes

SCM uses the following fixed ports on *managed nodes*, including the CMS:

Service	Port	Protocol	Used By	Configurable?
WBEM/ HTTP	5988 Inbound/Outbound	TCP	WBEM	No
WBEM/ HTTPS	5989 Inbound/Outbound	TCP	WBEM	No
RMI	2367 Inbound/Outbound	TCP	SCM Daemons	No
SNMP	161 Inbound/Outbound	UDP	SNMP	No
DCE RPC	135 Inbound (possibly others)	TCP	DMI	No
HTTP	2301 Inbound	TCP	ProLiant Web agent (Elm)	No
HTTPS	2381 Inbound	TCP	ProLiant Web agent (Elm)	No
RMI	Anonymous (see section below) Inbound/Outbound	TCP	SCM Daemons	Yes

Not all WBEM, SNMP, or DMI services may be present on every managed node.

Anonymous Ports

In addition to the fixed ports, SCM uses a number of anonymous TCP ports in the range assigned by the operating system. On a managed node, a maximum of 10 anonymous ports are required from the pool. On the CMS, the number of anonymous ports required depends on:

- the number of concurrent commands running
- the number of concurrent browser sessions open

An approximate formula for the maximum number of anonymous sockets required for the CMS is:

$$\text{number of required anonymous sockets} = 103 + (2 \times \text{concurrent commands}) + (5 \times \text{concurrent browser sessions})$$

For example, a typical use of SCM with two commands active concurrently and two browser sessions active concurrently would require the following anonymous sockets on the CMS:

$$103 + (2 \times 4) + (5 \times 2) = 121 \text{ anonymous sockets}$$

If required, the maximum and minimum anonymous socket numbers can be set for HP-UX and Linux.

- For HP-UX:

```
ndd -set /dev/tcp tcp_smallest_anon_port min_port
```

```
ndd -set /dev/tcp tcp_largest_anon_port max_port
```

- For Linux:

```
/sbin/sysctl -w net.ipv4.ip_local_port_range="min_port max_port"
```

where *min_port* and *max_port* delimit the desired anonymous port number ranges. Note that changes by these commands do not persist across a reboot. For more information, consult the appropriate manual pages for these commands. When setting the anonymous port ranges, be sure to also consider the anonymous port requirements of other applications running on the CMS and the managed nodes.

Increased Security Options

If you are in an environment where you need a higher level of security than what is provided by default with SCM, there are several things you can do to increase security.

Chapter 4, “Increasing Servicecontrol Manager Security,” on page 55 covers the following topics:

- “Replace Self-Signed Tomcat Certificates” on page 56
- “Enable WBEM Certificate Validation” on page 57
- “Encrypt Java RMI Transactions” on page 60
- “Disable the Tomcat Web Server” on page 61
- “Manage SCM Software” on page 62
- “Verify Security Dependencies” on page 63

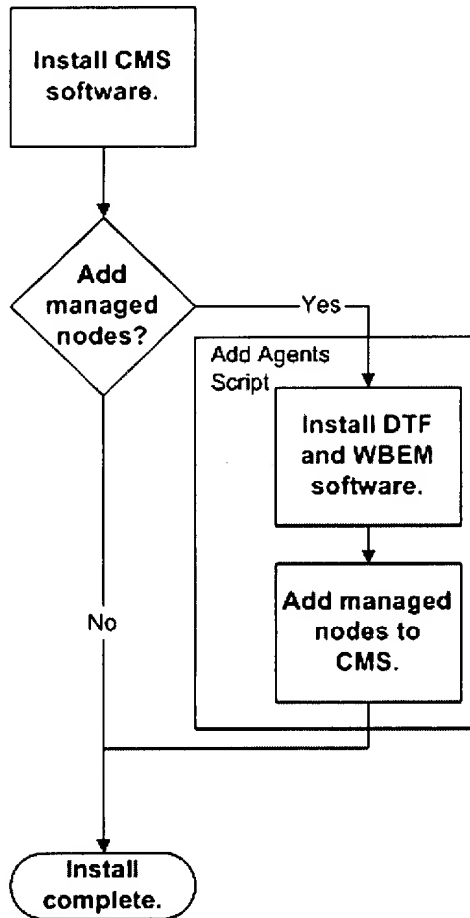
This chapter covers the following topics:

- “Installation Overview” on page 26
- “System Requirements” on page 28
- “Installing Servicecontrol Manager on HP-UX” on page 30
- “Installing Servicecontrol Manager on Linux” on page 33
- “Adding Managed Nodes” on page 37
- “Upgrading from Servicecontrol Manager 2.5 to 3.0” on page 41
- “Updating to Servicecontrol Manager 3.0 Version 3.00.04” on page 45
- “Removing Servicecontrol Manager” on page 46

Installation Overview

Installing a management domain involves installing the central management server (CMS), installing the DTF and WBEM agent software on the managed nodes, and adding the managed nodes to the CMS. Figure 2-1 presents a flow diagram of the install process.

Figure 2-1 **SCM Install Process**



Accessing the software

Servicecontrol Manager is available on the Web and with the HP-UX application releases.

To download SCM from the Web:

- Step 1.** Using a Web browser, go to the following URL:
- <http://software.hp.com/products/SCMGR/download.html>**
- Step 2.** Download all the appropriate software.

**Estimated
installation time**

The time it takes to install an SCM management domain will depend on the performance and load of the target systems during the install process and on your familiarity with the execution process. It will also depend on the size of the management domain that you are installing. Adding managed nodes with the `add_nodes` script can significantly reduce the installation time if you are installing a large management domain. The `add_nodes` script is discussed in the section “Adding Managed Nodes” on page 37.

System Requirements

For the latest system requirements, go to: <http://software.hp.com/products/SCMGR/>

CMS requirements The table below identifies the hardware and software requirements for an SCM central management server (CMS).

Operating System	<ul style="list-style-type: none">• HP-UX 11.0• HP-UX 11i v1 (B.11.11)• HP-UX 11i v2 (B.11.23)• Red Hat Linux 7.2 Professional• Red Hat Linux 7.3 Professional• SuSE Linux 8.0 Professional
Software	<ul style="list-style-type: none">• Java SDK version 1.4 or later• MySQL version 3.23• Tomcat version 4.1.12 or later• Required Patches - See the Servicecontrol Manager Release Notes for patch information.
Computer	<ul style="list-style-type: none">• HP Server - R Class or better recommended• Linux Server - Pentium III or better recommended
Free Disk Space	<ul style="list-style-type: none">• 110 MB for the SCM CMS and DTF agent (/opt)• 15 MB for MySQL (/var)• 500 MB minimum for data recommended (/var/opt)
RAM	256 MB
Swap Space	<ul style="list-style-type: none">• 200 MB incremental in addition to the server's previous minimum total swap space requirement• 500 MB minimum total swap space
Networking	static hostname resolution
Kernel Tuning	<ul style="list-style-type: none">• max_thread_proc = 150 for up to 32 nodes 250 for up to 64 nodes 10,000 for up to 1000 nodes• nkthread = 1000

Managed node requirements

The table below identifies the hardware and software requirements for an SCM managed node.

Operating System	<ul style="list-style-type: none"> • HP-UX 11.0 • HP-UX 11i v1 (B.11.11) • HP-UX 11i v2 (B.11.23) • Red Hat Linux 7.2 Professional • Red Hat Linux 7.3 Professional • SuSE Linux 8.0 Professional
Free Disk Space	100 MB for the SCM DTF agent (/opt)
Networking	static hostname resolution

Network Client

The table below identifies the software requirements for a network client accessing SCM through the graphical user interface.

Web Browser	<ul style="list-style-type: none"> • Microsoft® Internet Explorer version 6.0 or later • Mozilla version 1.2.1 or later • Netscape version 7.0 or later
Software	X server software (required for running X Windows tools)

To access the software for the supported Web browser versions, see the appropriate source listed below.

- For Microsoft Internet Explorer, go to <http://www.microsoft.com>
- For Mozilla on HP-UX, go to <http://www.hp.com/go/mozilla>
- For Mozilla on Windows or Linux, go to <http://www.mozilla.org>
- For Netscape, go to <http://www.netscape.com>

Installing Servicecontrol Manager on HP-UX

This section provides steps to successfully install the Servicecontrol Manager (SCM) central management server (CMS) on a server running a supported version of HP-UX. See “System Requirements” on page 28 to verify which versions of HP-UX are supported.

If you are installing SCM on Linux, see “Installing Servicecontrol Manager on Linux” on page 33.

Before You Install CMS Software on an HP-UX Server

Several dependent software packages need to be verified before you install SCM. Based on this information, you may be able to skip portions of the CMS install.

NOTE

If you need to remove Tomcat or MySQL, verify that it isn't being used by another application. If one or both of these applications cannot be removed, you must select a different server to be the CMS.

To verify dependent software packages:

- Step 1.** Verify that Java SDK version 1.4 is installed:

```
swlist T1456AA
```

If the correct version of Java SDK is already installed, you can skip installing it during the CMS software installation. If a different version is installed, multiple versions of Java SDK can coexist on the same HP-UX server.

- Step 2.** Verify that Tomcat version 4.1.12 is installed:

```
swlist hpuxwsTomcat
```

If the correct version of Tomcat is already installed, you can skip installing it during the CMS software installation. If a different version is installed, you need to remove it before installing SCM.

To remove Tomcat:

- a. Uninstall the Tomcat:

```
swremove hpuxwsTomcat
```

- b. Verify that Tomcat is removed:

```
swlist hpuxwsTomcat
```

- c. Remove or rename the following Tomcat directories if they exist:

```
/var/tomcat
```

```
/etc/tomcat
```

- Step 3.** Verify that MySQL version 3.23 is installed:

```
swlist mysql MySQL
```

NOTE

MySQL may have been installed from a tar file instead of an SD package. Look in /var and /opt to see if it is installed from a tar file.

If the correct version of MySQL is already installed, you can skip installing it during the CMS software installation. If a different version is installed, you need to remove it before installing SCM.

To remove MySQL:

- a. Uninstall the MySQL:

swremove MySQL

where *MySQL* is the bundle ID.

- b. Verify that MySQL is removed:

swlist MySQL

where *MySQL* is the bundle ID.

Installing CMS Software on an HP-UX Server

This installation process includes installing Java SDK, MySQL, and Tomcat in addition to SCM.

NOTE

This procedure assumes that the appropriate enablement patches have been installed on the server. For details about which patches are required and steps to install them, see the *Servicecontrol Manager 3.0 Release Notes* on the Web at:

<http://software.hp.com/products/SCMGR/download.html>

To install CMS software on an HP-UX server:

- Step 1.** Download the required depot files identified below or locate them on the network if they are already available. To download, go to:

<http://software.hp.com/products/SCMGR/download.html>

- **For HP-UX 11.00**

CMS and Agent Software: SCM.3.0_11.00_11.11.depot

- **HP-UX 11i v1**

CMS and Agent Software: SCM.3.0_11.00_11.11.depot

- **HP-UX 11i v2**

CMS and Agent Software: SCM.3.0_11.23.depot

- Step 2.** Register the depot files on the depot server:

swcopy -s filename.depot * @ directory

where *filename.depot* is the name of the depot file that you downloaded and *directory* is the directory where the files will be copied to.

Step 3. Install Java SDK if version 1.4 or later isn't installed on the system:

```
swinstall -s server:directory T1456AA
```

where *server* is the hostname of the depot server and *directory* is the location of the depot files on the depot server.

Step 4. Install Tomcat if version 4.1.12 isn't installed on the system:

```
swinstall -s server:directory hpuxwsTomcat
```

where *server* is the hostname of the depot server and *directory* is the location of the depot files on the depot server.

Step 5. Install MySQL if version 3.23 isn't installed on the system:

```
swinstall -x allow_incompatible=true -s server:directory MySQL
```

where *server* is the hostname of the depot server and *directory* is the location of the depot files on the depot server.

Step 6. Install Servicecontrol Manager:

```
swinstall -s server:directory B8339BA
```

Where *server* is the hostname of the depot server and *directory* is the location of the depot files on the depot server.

Step 7. Initialize and configure the CMS:

```
/opt/mx/bin/mxinitconfig -a server
```

Next Steps

Servicecontrol Manager is now installed. The next step is to install and add managed nodes, see "Adding Managed Nodes" on page 37 for details.

Installing Servicecontrol Manager on Linux

This section provides steps to successfully install the Servicecontrol Manager (SCM) central management server (CMS) on a server running a supported version of Linux. See “System Requirements” on page 28 to verify which versions of Linux are supported.

If you are installing SCM on HP-UX, see “Installing Servicecontrol Manager on HP-UX” on page 30.

The CMS install procedure for Linux utilizes a bin file (self-extracting tar files) to simplify the process. Using the bin files automatically installs all the rpm files in the correct order. You can extract the rpm files from the bin files and install them manually if preferred.

Before You Install CMS Software on a Linux Server

Before you install SCM, you need to verify which version of several dependent software packages are installed. Based on this information, you may be able to skip portions of the SCM install.

NOTE

If you need to remove Tomcat or MySQL, verify that it isn't being used by another application. If one or both of these applications cannot be removed, you must select a different server to be the CMS.

To verify dependent software packages:

Step 1. Verify that Tomcat version 4.1.12 is installed:

```
rpm -q tomcat4 xml-commons xml-commons-apis
```

If a different version is installed, you need to remove it.

To remove Tomcat:

a. Uninstall the Tomcat products:

```
rpm -e tomcat4 xml-commons xml-commons-apis
```

b. Verify that Tomcat is removed:

```
rpm -q tomcat4 xml-commons xml-commons-apis
```

c. Remove or rename the following Tomcat directories if they exist:

```
/var/tomcat
```

```
/etc/tomcat
```

NOTE

If you plan to install using the bin files, you may skip the remaining verification steps. See “Installing CMS Software on a Linux Server” on page 34 to continue with the installation.

Step 2. Verify that MySQL version 3.23 is installed:

```
rpm -qa | grep mysql
```

If the correct version of MySQL is already installed, you can skip installing it during the CMS software installation. If a different version is installed, you need to remove it before installing SCM.

To remove MySQL:

- a. Identify the MySQL product names including MySQL, MySQL server, MySQL shared, and MySQL client:

```
rpm -qa | grep mysql
```

- b. Uninstall the MySQL products that you identified in step a:

```
rpm -e mysql_product1 mysql_product2 mysql_product3
```

where *mysql_product1* *mysql_product2* *mysql_product3* are the names of each of the products.

- c. Verify that MySQL is removed:

```
rpm -qa | grep mysql
```

Step 3. Verify that Java SDK version 1.4 is installed:

```
rpm -q j2sdk
```

If the correct version of Java SDK is already installed, you can skip installing it during the manual CMS software installation. If a different version is installed, multiple versions of Java SDK can coexist on the same Linux server.

Installing CMS Software on a Linux Server

This installation process includes installing Java SDK, MySQL, and Tomcat in addition to SCM. To install the CMS software, you can either:

- automatically install the CMS software using the bin files
- manually install the CMS software using individual rpm files

To automatically install the CMS software on a Linux server:

Step 1. Download the required bin files identified below to the local file system or copy them from a network location if they are already available. To download, go to:

<http://software.hp.com/products/SCMGR/download.html>

- **For Red Hat Linux 7.2 and 7.3**

CMS Software: SCM.3.0_RH.7.2_7.3_mxserver.bin

Agent Software: SCM.3.0_RH.7.2_7.3_mxagent.bin

- **For SuSE Linux 8.0**

CMS Software: SCM.3.0_SuSE.8.0_mxserver.bin

Agent Software: SCM.3.0_SuSE.8.0_mxagent.bin

Step 2. Give all users permission to execute the bin files.

```
chmod +x *.bin
```

Step 3. Install SCM directly from the bin files:

- For Red Hat Linux 7.2 or 7.3:

SCM.3.0_RH.7.2_7.3_mxserver.bin

- For SuSE Linux 8.0:

SCM.3.0_SuSE.8.0_mxserver.bin

Step 4. Initialize and configure the CMS:

/opt/mx/bin/mxinitconfig -a server

To manually install the CMS software on a Linux server:

Step 1. Download the required bin files identified below to the local file system or copy them from a network location if they are already available. To download, go to:

<http://software.hp.com/products/SCMGR/download.html>

- **For Red Hat Linux 7.2 and 7.3**

CMS Software: **SCM.3.0_RH.7.2_7.3_mxserver.bin**

Agent Software: **SCM.3.0_RH.7.2_7.3_mxagent.bin**

- **For SuSE Linux 8.0**

CMS Software: **SCM.3.0_SuSE.8.0_mxserver.bin**

Agent Software: **SCM.3.0_SuSE.8.0_mxagent.bin**

Step 2. Give all users permission to execute the bin files.

chmod +x *.bin

Step 3. Extract the rpm files from the bin file.

mxfile.bin --keep --confirm

where *mxfile* is the name of the bin file.

Step 4. Respond negatively to the prompt to run scripts.

The extracted files will be placed in a subdirectory with the name of the bin file, *mxserver* or *mxagent*.

Step 5. Install the appropriate rpm files in the following order:

- **j2sdk-1.4.1_04-fcs-linux-i386.rpm**
- **tomcat4-4.1.12-1e.2jpp.noarch.rpm**
- **xml-commons-1.0-0.b2.1jpp.noarch.rpm**
- **xml-commons-apis-1.0-0.b2.1jpp.noarch.rpm**
- **For Red Hat 7.2 only:**
 - **mysql-3.23.36-1.i386.rpm**
 - **mysql-server-3.23.36-1.i386.rpm**
 - **mysqlclient9-3.23.22-4.i386.rpm**
- **For Red Hat 7.3 only:**
 - **mysql-3.23.49-3.i386.rpm**

- mysql-server-3.23.49-3.i386.rpm
- mysqlclient9-3.23.22-4.i386.rpm
- For SuSE 8.0 only:
 - mysql-3.23.48-35.i386.rpm
 - mysql-shared-3.23.48-35.i386.rpm
 - mysql-client-3.23.48-35.i386.rpm
- mxagent-B.03.00.04.i386-1.rpm
- mxrepository-B.03.00.04.i386-1.rpm
- mxcms-B.03.00.04.i386-1.rpm

Step 6. Initialize and configure the CMS:

```
/opt/mx/bin/mxinitconfig -a server
```

Next Steps

Servicecontrol Manager is now installed. The next step is to add managed nodes, see “Adding Managed Nodes” on page 37 for details.

Adding Managed Nodes

This procedure walks you through adding managed nodes to a new management domain. Managed node systems must be running a supported version of HP-UX or Linux. Adding a managed node involves:

- setting the agent configuration password
- verifying the default WBEM and SNMP usernames and passwords
- verifying the default authorizations
- installing the DTF agent and WBEM software
- configuring the managed node
- adding the new node to the management domain
- adding the new node to the Managed Nodes node group
- testing the new node

To add a managed node, you can either:

- automatically add a group of managed nodes using the `add_nodes` script
- manually add managed nodes

The `add_nodes` script walks you through adding managed nodes. Using this script will significantly reduce the time and complexity of adding managed nodes.

NOTE

The SCM software must be installed on the central management server (CMS) prior to adding a managed node, and the CMS must be available on the network. See “Installing Servicecontrol Manager on HP-UX” on page 30 or “Installing Servicecontrol Manager on Linux” on page 33 for details.

NOTE

The CMS and managed nodes must be time-synchronized to prevent authentication failures. The communication time limit is 20 minutes, and exceeding this limit causes authentication failures.

NOTE

This procedure assumes that SNMP is configured on each managed node. If you want to use SNMP tools with SCM, SNMP should be configured prior to adding managed nodes. By default, SNMP is configured on HP-UX systems.

To automatically add managed nodes:

Step 1. Log on to the CMS as root.

Step 2. Run the `add_nodes` script.

```
/opt/mx/sbin/add_nodes node1 node2 node3...
```

where `node1 node2 node3...` is the list of hostnames or IP addresses for the nodes you want to add.

Step 3. Verify the new nodes by testing the configuration:

```
/opt/mx/bin/mxexec -t df -n node1 node2 node3...
```

where `node1 node2 node3...` is the list of hostnames or IP addresses for the nodes you added.

To manually add managed nodes:

Step 1. Log on to the CMS as root.

Step 2. Verify the location of the SCM agent software.

You located and/or downloaded this software at the same time that you located the CMS software during the CMS install process.

Step 3. View the agent configuration password (MxConfigPassword):

```
mxpassword -l
```

Remember this password because it is used to validate communication between the CMS and managed node during the adding managed nodes procedure. Change the password to something easier to remember if desired:

```
mxpassword -m -x MxConfigPassword=new_password
```

where *new_password* is the new password.

Step 4. By default, SCM expects a WBEM username of *guest* and a password of *guest*. The expected username and password information is accessible on the CMS using the `mxnodesecurity` command.

An account with the expected WBEM username and password must exist on each managed node. Change the default username and password if desired:

```
/opt/mx/bin/mxnodesecurity -a -p wbem -c username:password
```

where *username* is the new username and *password* is the new password.

Step 5. By default, SCM expects an SNMP username of *public* and a password of *public*. The expected username and password information is accessible on the CMS using the `mxnodesecurity` command.

An account with the expected username and password must exist on each managed node. Change the default username and password if desired:

```
/opt/mx/bin/mxnodesecurity -a -p snmp -c username:password
```

where *username* is the new username and *password* is the new password.

Step 6. By default, all new nodes are added to the Managed Nodes node group. Verify that this node group exists:

```
mxngroup
```

If the Managed Nodes node group isn't listed, you need to create the node group:

```
mxngroup -a -g "Managed Nodes"
```

Step 7. By default, all new nodes inherit the Managed Node node group authorizations. Identify the authorizations for this node group:

```
mxauth -lt
```

By default, root should be authorized with the Master Role for this node group. To authorize root with the Master Role for the Managed Nodes node group:

```
mxauth -a -g "Managed Nodes" -R "Master Role" -u root
```

Step 8. Log on to one of the managed nodes as root.

NOTE Step 8 to step 11 will need to be completed on each managed node separately.

Step 9. Install the SCM DTF agent and WBEM software on the managed node:

- For HP-UX (all versions):

```
swinstall -s server:directory B8339BA.SysMgmtAgent B8465BA
```

where *server* is the hostname of the depot server and *directory* is the location of the depot files on the depot server.

NOTE You must have appropriate permissions to execute the following bin files. Use the `chmod +x` command to change the file permissions.

- For Red Hat Linux 7.2 or 7.3:

```
SCM.3.0_RH.7.2_7.3_mxagent.bin
```

- For SuSE Linux 8.0:

```
SCM.3.0_SuSE.8.0_mxagent.bin
```

Step 10. Configure the managed node:

```
/opt/mx/bin/mxagentconfig -a -n cms -p password
```

where *cms* is the hostname of the CMS and *password* is the MxConfigPassword that you verified earlier.

Step 11. Configure WBEM and start the cimserver on the managed node:

```
/opt/wbem/sbin/cimconfig -s enableRemotePrivilegedUserAccess=true -p
```

```
/opt/wbem/sbin/cimserver
```

Step 12. Repeat step 8 to step 11 for the remaining managed nodes.

Step 13. Return to the CMS, and log on as root.

Step 14. Add the new nodes to the management domain:

```
/opt/mx/bin/mxnode -a -i node1 node2 node3...
```

where *node1 node2 node3...* is the list of hostnames or IP addresses for the nodes you added.

Step 15. Add the new nodes to the Managed Nodes node group:

```
/opt/mx/bin/mxngroup -m -g "Managed Nodes" -n node1 node2 node3...
```

where *node1 node2 node3...* is the list of hostnames or IP addresses for the nodes you added.

Step 16. Verify the new nodes by testing the configuration:

```
/opt/mx/bin/mxexec -t df -n node1 node2 node3...
```

Adding Managed Nodes

where *node1 node2 node3 . . .* is the list of hostnames or IP addresses for the nodes you added.

Upgrading from Servicecontrol Manager 2.5 to 3.0

The SCM upgrade will install the 3.0 version of SCM and migrate your SCM data to be compatible with SCM 3.0. The upgrade installation migrates all custom data including:

- users
- nodes
- node groups
- tools
- roles
- authorizations

Multiple versions of SCM cannot coexist on the same system.

NOTE	You must be running SCM 2.5 to upgrade to 3.0. If you are running a version of SCM earlier than 2.5, you must upgrade to 2.5 before upgrading to 3.0.
-------------	---

NOTE	SCM 3.0 agents are only compatible with an SCM 3.0 central management server (CMS). SCM 2.5 agents must be upgraded to 3.0 before you can manage them with a CMS running SCM 3.0.
-------------	---

NOTE	Linux managed nodes must be installed as new nodes. This procedure includes steps to remove existing SCM software from Linux managed nodes and install SCM 3.0.
-------------	---

CAUTION	The following directories are deleted during the SCM upgrade:
----------------	--

`/var/mx/`
`/etc/opt/mx/`
`/opt/webadmin/mx/`
`/opt/mx/`

If you have stored files in these directories, you need to relocate those files prior to upgrading, or the data will be lost.

To upgrade from SCM 2.5 to 3.0:

Step 1. Verify that SCM 2.5 is running on the system.

```
swlist B8339BA
```

If SCM 2.5 isn't running, start it.

```
/sbin/init.d/ServCtlMgr start
```

Step 2. Back-up your SCM data by copying the output of the mx commands into a file.

```
mxnode -ln > /directory/mxnode.scm25
```

```
mxngroup -ln > /directory/mxngroup.scm25
```

```
mxauth -lf > /directory/mxauth.scm25
```

```
mxuser -lf > /directory/mxuser.scm25
```

```
mxtool -lf > /directory/mxtool.scm25
```

```
mxrole -lt > /directory/mxrole.scm25
```

where *directory* is a directory that won't be deleted during the installation upgrade.

- Step 3.** Install the software on the CMS by following the instructions in the section “Installing Servicecontrol Manager on HP-UX” on page 30.

CAUTION

When upgrading the CMS, do not install the SCM software with other products at the same time.

- Step 4.** Check the `swagent.log` file on the CMS for errors:

```
/var/adm/sw/swagent.log
```

- Step 5.** Remove Debian 2.2 managed nodes if applicable. Debian is no longer a supported operating system.

- a. Remove the agent software on each managed node:

```
rpm -e mxagent
```

- b. Remove the agent from the CMS configuration:

```
mxmode -r -n node
```

where *node* is the hostname of the managed node.

- Step 6.** Upgrade existing HP-UX managed nodes:

- a. Upgrade the SCM software on each HP-UX node and install the WBEM agent:

```
swinstall -s server:directory B8339BA.SysMgmtAgent B8465BA
```

where *server* is the hostname of the depot server and *directory* is the location of the depot files on the depot server.

- b. Configure the managed node:

```
/opt/mx/bin/mxagentconfig -a -n cms -p password
```

where *cms* is the hostname of the CMS and *password* is the MxConfigPassword that you verified earlier.

- c. Configure WBEM and start the cimserver on each managed node:

```
/opt/wbem/sbin/cimconfig -s enableRemotePrivilegedUserAccess=true -p
```

```
/opt/wbem/sbin/cimserver
```

- Step 7.** Remove and add existing Linux managed nodes:

- a. Remove any existing SCM software from the Linux managed nodes. Follow the steps in “Removing Servicecontrol Manager” on page 46.

- b. Add the Linux nodes by following the instructions in “Adding Managed Nodes” on page 37. This step can be performed in conjunction with adding new managed nodes in the following step.

- Step 8.** Add new managed nodes by following the instructions in “Adding Managed Nodes” on page 37.

Additional Suggested Removal and Clean-up Tasks

There are several additional tasks you may want to perform to fully remove SCM 2.5 from your CMS system.

Remove Netscape Directory Server (NDS)

NDS provided the repository for SCM 2.5, and it is not removed during the upgrade in case you need to extract data from it after you upgrade. SCM 3.0 uses MySQL instead of NDS for the repository. Once you have verified that all your data successfully converted over to SCM 3.0, you can remove the NDS.

CAUTION

Removing NDS deletes the data in the SCM 2.5 repository. If the data is important, make sure it is backed up first.

To remove Netscape Directory Server:

- Step 1.** Uninstall NDS by entering the commands:

```
cd /var/opt/netscape/server4
./uninstall
```

- Step 2.** Select **ALL** to uninstall the entire NDS.

- Step 3.** Remove the NDS product by running the command:

```
swremove J4258BA
```

- Step 4.** Check the output for errors. If errors are reported, refer to the `swagent.log` file:

```
/var/adm/sw/swagent.log
```

Manually Converting a Tool From SCM 2.5 to 3.0

When you upgrade from SCM 2.5 to 3.0, your tools should automatically be converted from a TDEF file to a new XML tool definition file. If you need to manually convert tools after the upgrade, you can use the following procedure.

To manually convert a tool

- Step 1.** Create the XML file from the TDEF using the conversion tool:

```
/opt/mx/1bin/def2xml -t tdef_filename xml_filename
```

where `tdef_filename` is the name of the original TDEF file and `xml_filename` is the name of the new XML file.

- Step 2.** Add the tool to SCM:

```
mxtool -a -f xml_filename
```

where `xml_filename` is the name of the new XML file.

- Step 3.** Verify the tool:

```
mxtool -ld -t "Tool Name"
```

where *Tool Name* is the name of the new tool.

Updating to Servicecontrol Manager 3.0 Version 3.00.04

Complete this procedure to update earlier versions of SCM 3.0 to version 3.00.04.

To update to SCM 3.0 version 3.00.04:

- Step 1.** Back-up your SCM data by copying the output of the `mx` commands into a file.

```
mxnode -ln > /directory/mxnode.scm30
mxngroup -ln > /directory/mxngroup.scm30
mxauth -lf > /directory/mxauth.scm30
mxuser -lf > /directory/mxuser.scm30
mxtool -lf > /directory/mxtool.scm30
mxrole -lt > /directory/mxrole.scm30
```

where *directory* is a directory that won't be deleted during the installation upgrade.

- Step 2.** Install the software on the CMS:

- For HP-UX:

```
swinstall -s server:directory B8339BA
```

where *server* is the hostname of the depot server and *directory* is the location of the depot files on the depot server.

- For Red Hat Linux 7.2 or 7.3:

```
SCM.3.00.04_RH.7.2_7.3_mxserver.bin
```

- For SuSE Linux 8.0:

```
SCM.3.00.04_SuSE.8.0_mxserver.bin
```

CAUTION

When updating the CMS, do not install the SCM software with other products at the same time.

- Step 3.** Check the `swagent.log` file on the CMS for errors:

```
/var/adm/sw/swagent.log
```

- Step 4.** Verify that SCM processes are running:

```
ps -ef |grep -e mx -e java
```

- If `tomcat` is not listed, start it:

```
/sbin/init.d/mxtomcat start
```

- If `mxagent`, `mxdtf` and `mxdomainmgr` are not listed, start SCM:

```
/opt/mx/bin/mxstart
```

Removing Servicecontrol Manager

You can either remove the SCM software or just remove the SCM configuration.

CAUTION

Removing the SCM software or removing the SCM configuration will delete all custom information in the SCM repository.

You can also remove a managed node from a CMS's management domain without removing the SCM agent on the node.

To remove SCM including the repository data:

Step 1. Remove the software from the CMS:

- For HP-UX:

```
swremove B8339BA
```

- For Linux:

```
rpm -e mxcms
```

```
rpm -e mxrepository
```

```
rpm -e mxagent
```

Step 2. Remove the software from the managed nodes:

- For HP-UX:

```
swremove B8339BA
```

- For Linux:

```
rpm -e mxagent
```

To remove the SCM configuration without removing the software:

Remove the configuration from the CMS or a managed node:

```
mxinitconfig -r [server|agent|all]
```

To remove a managed node from a management domain:

Remove a CMS from managing a node:

```
mxagentconfig [-F] -r -n cms
```

where *cms* is the hostname of the CMS. The optional [-F] force option is used in cases where the CMS is not available on the network.

If this is your first time using HP Servicecontrol Manager (SCM), this chapter provides procedures to familiarize you with the SCM features using the graphical user interface and the command line interface.

This chapter covers the following topics:

- “Types of SCM Users” on page 48
- “Getting Started Using SCM” on page 49
- “Getting Started Administering SCM” on page 52

Types of SCM Users

As an SCM user, you will be using it in at least one of the following capacities:

- using SCM to manage network resources
- administering SCM to enable other users to manage network resources

Users who administer SCM must be assigned the trusted user privilege. The features and benefits of SCM will vary based on how you use it.

Users who manage network resources with SCM

SCM offers you a choice of management interfaces: a Web-enabled graphical user interface (GUI) or a command line interface (CLI). You can access SCM from any network client that is running a supported Web browser. Using either interface, SCM enables you to simultaneously launch management tasks across multiple servers, which increases your efficiency.

For steps to get started using SCM, see “Getting Started Using SCM” on page 49.

Trusted users who administer SCM

SCM enables you to easily add custom tools, including scripts or commands, that users can execute across multiple systems simultaneously. You can also add existing HP-UX, Linux, and Windows management tools to SCM.

In addition, SCM uses role-based management to assign access to certain tools for specific managed nodes or node groups. Role-based access reduces error-caused downtime by allowing delegation of administrative tasks without a proliferation of root privileges. In addition, SCM's audit logging capabilities ensures accountability for actions and tracks changes across the IT environment by recording all task information.

For steps to get started using SCM, see “Getting Started Administering SCM” on page 52.

Getting Started Using SCM

Get started using SCM by familiarizing yourself with how to log on, select a node, and execute a tool.

This procedure walks you through launching several different types of tools from the graphical user interface and the command line interface. This procedure is optional but recommended for new users.

To get started using SCM:

Step 1. Log on to the SCM graphical user interface.

- a. Open a Web browser on any network client that is connected to your company intranet.
- b. Access the log on screen by navigating to:
`https://hostname:50000/`
where *hostname* is the hostname of the central management server (CMS).
- c. Enter your **User name** and **Password**.
- d. Click **Log On**.

The nodes list appears in the workspace.

Step 2. Select an HP-UX or Linux node with the DTF protocol.

- a. From the **Nodes** tab menu, select **All Nodes** to load the nodes list in the workspace.
- b. Select or clear the check boxes beside the nodes as necessary.

The **Tools** tab menu replaces the **Nodes** tab menu after you select a node.

Step 3. Execute the **df** tool on the selected target node.

- a. From the **Tools** tab menu, expand **General Tools** and select **df**.

If this tool isn't available, your authorizations may not be associated with this tool, or the node selected isn't compatible with this tool.

The tool launch page displays in the workspace.

- b. Click **Execute** on the tool launch page.

The **View Task Results** screen displays in the workspace.

- c. Verify the **Status** is Complete, and view the results on the **Stdout** tab.

If the **Status** is Error, view the error information on the **Stderr** tab.

Step 4. Select an HP-UX node with the DTF protocol.

- a. From the **Nodes** tab menu, select **All Nodes** to load the nodes list in the workspace.
- b. Select or clear the check boxes beside the nodes as necessary.

The **Tools** tab menu replaces the **Nodes** tab menu after you select a node.

Step 5. Execute the **Accounts for Users and Groups** tool on the selected target node.

- a. From the **Tools** tab menu, expand **System Administration** and select **Accounts for Users and Groups**.

If this tool isn't available, your authorizations may not be associated with this tool, or the node selected isn't compatible with this tool.

The tool launch page displays in the workspace.

- b. Open an X server or server emulator on the network client where you want to display the tool.
- c. On the tool launch page, enter the **Device for X Window display** as **network_client:0.0** where *network_client* is the hostname or IP address of the network client with the X server running.
- d. Click **Execute** on the tool launch page.
- e. View the **Accounts for Users and Groups** tool in the X Window.

Step 6. Select a node with the WBEM protocol.

- a. From the **Nodes** tab menu, select **All Nodes** to load the nodes list in the workspace.
- b. Select or clear the check boxes beside the nodes as necessary.

The Tools tab menu replaces the Nodes tab menu after you select a node.

Step 7. Execute the **View Properties** tool on the selected target node.

- a. From the **Tools** tab menu, expand **View** and select **View Properties**.

If this tool isn't available, your authorizations may not be associated with this tool, or the node selected isn't compatible with this tool.

The **View Properties** tool displays in the workspace.

- b. Select the **Identity** tab, **Status** tab, or **Configuration** tab to view details about the target node.

Step 8. View a log of the tasks you just performed.

- a. Execute the **View Tasks** tool by selecting it from the **Tools** tab menu.
- b. Click any task in the list to **View Task Results** in the lower half of the page.

Step 9. Log off of the SCM graphical user interface by clicking the >> **Log Off** link in the top right-hand corner to the page.

Step 10. Close the browser.

Step 11. Log on to the CMS directly or using an SSH secure shell.

When you log on to the CMS, you are granted authorizations based on your operating system login.

Step 12. Execute the **df** tool on the same HP-UX or Linux target node that you selected in step 2.

- a. Execute the tool:

```
mxexec -t df -n node
```

where *node* is the hostname or IP address of the target node.

- b. View the results displayed on the screen.

Step 13. Execute the Accounts for Users and Groups tool on the same HP-UX target node that you selected in step 4.

a. Type the command:

```
mexec -t "Accounts for Users and Groups" -n node
```

where *node* is the hostname or IP address of the target node.

b. View the results displayed on the screen.

Step 14. Execute the View Properties tool on the same target node with WBEM installed that you selected in step 6.

a. Type the command:

```
mexec -t "View Properties" -n node
```

where *node* is the hostname or IP address of the target node.

b. View the results displayed in the Web browser.

Additional Information

For more information about using SCM, see the SCM online help. Topics available in the online help including:

- navigating SCM
- performing tasks
- viewing the management home page
- viewing node properties
- viewing the SCM audit log
- customizing the nodes list

Getting Started Administering SCM

Get started administering SCM by familiarizing yourself with how to add a tool. To administer SCM, you must be a trusted user.

This procedure walks you through adding a custom tool and executing the tool from the command line interface and the graphical user interface.

To get started administering SCM:

Step 1. Log on to the central management server (CMS) as a trusted user.

Step 2. Create a XML tool definition file for a new command tool.

a. Open a text editor and paste the following tool definition file example into the file.

```
<?xml version="1.0" encoding="UTF-8" ?>
<tool-list>
  <ssa-command-tool name="Test Find tmp">
    <category>General Tools</category>
    <description>Find all the tmp directory and files</description>
    <comment> Example Tool </comment>
    <include-filter type="os">
      <node-filter name="OSName" operator="eq" value="HPUX"/>
    </include-filter>
    <include-filter type="os">
      <node-filter name="OSName" operator="eq" value="LINUX"/>
    </include-filter>
    <ssa-block>
      <command command-type="stdout" log="true">
        find / -name tmp</command>
      </ssa-block>
    </ssa-command-tool>
```

b. Replace **tmp** with **mx**.

There are three instances that need to be changed.

Step 3. Save the tool definition file as **testtool.xml**.

Step 4. Copy the tool definition file to:

```
/var/opt/mx/tools
```

Step 5. Add the tool to SCM:

```
mxtool -a -f testtool.xml
```

Step 6. Execute the tool to test it:

```
mxexec -t "Test Find mx" -n node
```

where *node* is the hostname of an authorized target node.

Step 7. Log on to the SCM graphical user interface.

a. Open a Web browser on any network client that is connected to your company intranet.

- b. Access the log on screen by navigating to:
`https://hostname:50000/`
where *hostname* is the hostname of the CMS.
- c. Enter your **User name** and **Password**.
- d. Click **Log On**.

Step 8. Select an HP-UX or Linux node with the DTF protocol.

- a. From the **Nodes** tab menu, select **All Nodes** to load the nodes list in the workspace.
- b. Select or clear the check boxes beside the nodes as necessary.

The **Tools** tab menu replaces the **Nodes** tab menu after you select a node.

Step 9. Run the tool from the graphical user interface.

- a. From the **Tools** tab menu, expand **General Tools** and select **Test Find mx**.
The tool launch page displays in the workspace.

- b. Click **Execute** on the tool launch page.

The **View Task Results** screen displays in the workspace.

- c. Verify the **Status** is Complete, and view the results on the **Stdout** tab.

If the **Status** is Error, view the error information on the **Stderr** tab.

Step 10. Remove the tool from SCM:

```
mxtool -r -f testtool.xml
```

NOTE

For additional information about XML tool definition files including examples of different tool types, see the reference section in the SCM online help.

Additional Information

For more information about administering SCM, see the SCM online help. Topics available in the online help including:

- adding authorizations
- adding and editing nodes or node groups
- adding and editing users
- adding and editing roles
- adding and removing tools
- managing and configuring the SCM audit log
- maintaining the SCM repository

Getting Started with SCM

Getting Started Administering SCM

Increasing Servicecontrol Manager Security

If you are in an environment where you need a higher level of security than what is provided by default with SCM, there are several things you can do to increase security.

This chapter covers the following topics:

- “Replace Self-Signed Tomcat Certificates” on page 56
- “Enable WBEM Certificate Validation” on page 57
- “Encrypt Java RMI Transactions” on page 60
- “Disable the Tomcat Web Server” on page 61
- “Manage SCM Software” on page 62
- “Verify Security Dependencies” on page 63

Replace Self-Signed Tomcat Certificates

Replacing the Tomcat self-signed certificate with a certificate authority signed (CA-signed) certificate on your CMS and your managed nodes will increase your security. You can purchase a CA-signed certificate from a third party certificate authority, or you can act as your own certificate authority.

This will increase SCM security if you are accessing SCM from a Web browser. It guarantees the authenticity of the Web pages, and it virtually eliminates the possibility of unauthorized data interceptions, unauthorized access to SCM, or unauthorized changes to your transactions. It also prevents the possibility of spoofing.

This security enhancement uses the Java keytool from Sun Microsystems. For more information on the keytool, go to <http://java.sun.com> and search for **summary of security tools**.

To replace the self-signed certificates:

Step 1. Log on to the CMS as root.

Step 2. Identify the MxKeystorePassword:

```
mxpassword -l -x MxKeystorePassword
```

Step 3. Generate a request for the Tomcat certificate that is placed in the keystore:

```
keytool -certreq -alias tomcat -keystore  
/etc/opt/mx/config/security/certificates -keypass password
```

where *password* is the MxKeystorePassword.

Step 4. Submit the output to a Certificate Authority to get a CA-signed server certificate.

Step 5. Create the new Tomcat keytool associated with the CA-signed server certificate:

```
keytool -import -alias tomcat -file ca_certificate -keystore  
/etc/opt/mx/config/security/certificates -keypass password
```

where *ca_certificate* is the filename for the new certificate and *password* is the MxKeystorePassword.

Enable WBEM Certificate Validation

By default, all WBEM transactions are encrypted, but the identity of the managed node is not validated. Certificates passed from target nodes are automatically trusted. Enabling certificate validation will increase the level of security for WBEM transactions. You can use self-signed certificates for medium security or CA-signed certificates for high security. The certificate manager inspects credentials for each transaction and either approves or denies the WBEM data exchange based on the credentials.

This security enhancement uses the Java `keytool` from Sun Microsystems. For more information on the `keytool`, go to <http://java.sun.com> and search for **summary of security tools**.

NOTE

Additional information about **HP WBEM Services** is available on the Web at:

<http://docs.hp.com/hpux/netsys/index.html>

You can use:

- self-signed certificates for a *medium* security level
- CA-signed certificates for a *high* security level

The self-signed certificates are generated by WBEM on each managed node when SSL is enabled. See the appropriate procedure to enable WBEM certificate validation for your certificate type.

To enable WBEM certificate validation with self-signed certificates:

Step 1. Log on to the CMS as `root`.

Step 2. Identify the `MxKeystorePassword`:

```
mxpassword -l -x MxKeystorePassword
```

Step 3. Create a copy the self-signed certificate on a managed node:

```
/opt/wbem/sbin/openssl x509 -in /var/opt/wbem/server.pem -out node.cer
```

where `node` is the hostname of the managed node.

Step 4. Securely copy the certificate to the `/etc/opt/mx/config/security/` directory on the CMS.

Step 5. Import the certificate into the trust store on the CMS:

```
keytool -import -alias node -file node.cer -keystore  
/etc/opt/mx/config/security/certificates -keypass password
```

where `node` is the hostname of the managed node and `password` is the `MxKeystorePassword`.

Step 6. Repeat this process for each managed node running WBEM.

Step 7. Edit the WBEM configuration files on the CMS to enable certificate validation. The files are located at:

- `/opt/hpwebadmin/bin/cim.properties`

- `/etc/opt/mx/config/collectors/cimclient.properties`

Comment out the following line that sets the trust manager in each file.

`TrustManager=orig.snia.wbemcmd.xml.DontValidateCertificate`

Step 8. Restart SCM and Tomcat on the CMS:

`/opt/mx/bin/mxstop`

`/opt/mx/bin/mxstart`

To enable WBEM certificate validation with CA-signed certificates:

NOTE	You must have a certificate server available on the network to use CA-signed certificates.
-------------	--

Step 1. Log on to the CMS as root.

Step 2. Identify the MxKeystorePassword:

`mxpassword -l -x MxKeystorePassword`

Step 3. Generate a CA-signed certificate on the certificate server, save it as `ca_certificate.cer`.

Step 4. Securely copy the generated CA certificate to the `/etc/opt/mx/config/security/` directory on the CMS.

Step 5. Import the CA-signed certificate into the trust store on the CMS:

`keytool -import -alias caroot -file ca_certificate.cer -keystore
/etc/opt/mx/config/security/certificates -keypass password`

where *password* is the MxKeystorePassword.

Step 6. On a managed node that is running WBEM, generate a certificate request to be signed by CA on the certificate server.

`/opt/wbem/sbin/openssl req -new -key /var/opt/wbem/server.pem -out
cert.csr -config /var/opt/wbem/ssl.cnf`

Step 7. Securely copy the generated certificate request from the managed node to the certificate server.

Step 8. Retrieve the signed certificate in base64 x509 format.

Step 9. Replace the certificate on the managed node with the new certificate generated from the certificate server. The certificate on each node is at `/var/opt/wbem/server.pem`.

Step 10. Restart WBEM on the managed node:

`kill -9 cimserver_pid`

Step 11. Repeat steps 6-10 for each managed node running WBEM.

Step 12. Edit the WBEM configuration files on the CMS to enable certificate validation. The files are located at:

- `/opt/hpwebadmin/bin/cim.properties`

- `/etc/opt/mx/config/collectors/cimclient.properties`

Comment out the following line that sets the trust manager in each file.

`TrustManager=orig.snia.wbemcmd.xml.DontValidateCertificate`

Step 13. Restart SCM and Tomcat on the CMS:

`/opt/mx/bin/mxstop`

`/opt/mx/bin/mxstart`

Encrypt Java RMI Transactions

Java RMI transactions can be encrypted using the IP Security Protocol (IPSec) to increase security on RMI transactions. IPSec provides an infrastructure to allow secure communications including authentication, integrity, and confidentiality over IP-based networks between systems and devices that implement the IPSec family of protocol standards. HP provides an IPSec software package for the HP-UX operating system. This product allows the encrypted/confidential use of DTF tools and X applications running on the managed nodes from the CMS.

Information about IPSec is available at:

<http://www.hp.com/products1/unix/operating/security/ipsec.html>

To install and configure IPSec, see *Installing and Administering HP-UX IPSec* at:

<http://docs.hp.com/hpux/internet/index.html#IPSec/9000>

Disable the Tomcat Web Server

For increased security, the Web server on the CMS can be shut down when it is not needed. This will prevent it from responding to any Web-based requests.

The SCM graphical user interface is dependent on the Web server. SCM operations can still be performed from the command line on the CMS when the Web server is shut down.

To shut down the Web server:

- For HP-UX: `/sbin/init.d/mxtomcat stop`
- For Linux: `/etc/init.d/mxtomcat stop`

To restart the Web server:

- For HP-UX: `/sbin/init.d/mxtomcat start`
- For Linux: `/etc/init.d/mxtomcat start`

Manage SCM Software

Inspect the Audit Log Regularly

The SCM audit log contains a record of all tasks performed by SCM users on all managed nodes. This log should be inspected regularly for unexpected use of sensitive tools or for access to sensitive managed nodes. See *administering SCM - audit log* in the SCM online help for more information about the audit log.

Restrict root access on the CMS

It is essential to SCM security to restrict root access on the CMS. A user logged in as root can change the SCM configuration, add authorizations for others to run tools, and can run any tool on any managed node. To reduce the risk of unauthorized root access on the CMS, enforce strict password selection and change policies.

Change Generated Passwords

At installation time, SCM generates four passwords used for purposes described below. These passwords are assigned randomly generated values at least ten characters long when SCM is installed. For improved security, these passwords should be changed immediately after installation to a different value at least ten characters long. The `mxcpassword` command is used to display or change the values for these passwords. See the *mxcpassword* manual page for details.

- There are two passwords that restrict access to the SCM database through MySQL.
 - The `DBAdminPassword` is analogous to the root password under HP-UX, and it protects all access to the databases under the control of MySQL.
 - The `MxDBUserPassword` protects access to just the SCM database under MySQL.
- The `MxConfigPassword` is used to provide DTF Agent and CMS authentication. For convenience, this value should be changed before adding any managed nodes. If it is changed after adding managed nodes, all the DTF agents on the managed nodes will need to be re-authenticated using the `mxagentconfig` command.
- The `MxKeystorePassword` is used for the Tomcat certificate keystore. If it is changed, you need to restart the Tomcat Web server using the command on page 61.

Closely Manage SCM Authorizations

Consider carefully the implications of allowing an SCM user to be a trusted user or assigning a user to the master role on the CMS.

- An SCM trusted user can potentially run any tool on any managed node, including the CMS.
- An SCM user assigned the master role on the CMS, can run any tool on the CMS.

In addition, the SCM model for allowing tools to be developed by non-trusted users requires that the user have the master role on the managed node being used to develop the tool. Do not use the CMS node for this purpose.

Verify Security Dependencies

Software Security Dependency

SCM security is dependent on the security of the products and technologies described in this chapter. A threat to the security of these dependencies is a threat to the security of SCM.

To minimize these threats, always apply the latest patches and updates available to combat known exploits. For this purpose, it is helpful to run the Security Patch Check tool on the HP-UX CMS and all HP-UX managed nodes. This tool helps improve security by recommending patches for security vulnerabilities in installed software. See the **Security Management** tool category in SCM for tools to facilitate this.

Network Security Dependency

Use of SCM on a network without a hardware or software firewall is not recommended. SCM does not guard against denial of service attacks. For increased network security, use a separate management LAN, suitably walled off from other networks.

Glossary

agent *See management agent*

authorization triplet A mapping of the authorization relationship between a user, a role, and a node or node group.

banner The section of the graphical user interface at the top of the screen that provides access to SCM help and other resources.

central management server CMS

A node in the management domain that executes the SCM software. All central operations within SCM are initiated from this node.

command line interface CLI

The set of commands that can be executed directly from the operating system's command shell.

certificate authority A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.

digital signatures A technology used to validate a transaction's sender. This technology uses private-keys to digitally sign the data, and public-keys to verify the sender.

distributed task facility DTF

A management application that manages the remote execution of tasks on managed nodes.

document type definition DTD

A file that identifies the elements and attributes that can be used to create the content of an XML document. It identifies where each element is allowed and which elements can appear within other elements.

extensible markup language XML

A simplified subset of Standard Generalized Markup Language (SGML) that offers extensible data modeling capabilities.

graphical user interface GUI

A program interface that takes advantage of the computer's graphics capabilities to make the program easier to use. SCM's GUI is Web-enabled and displays in a Web browser.

group *See node group*

IP Security Protocol IPSEC

An infrastructure to allow secure communications (authentication, integrity, confidentiality) between systems and devices that implement the IPsec family of protocol standards.

Java Remote Method Invocation RMI

A set of protocols that enable Java objects to communicate remotely with other Java objects.

managed node *See node*

management agent A daemon process or application running on a managed node. It receives and executes requests from the CMS on the managed node.

management domain A collection of resources called managed nodes that have been placed under the control of the SCM. Each central management server is responsible for a management domain. The managed nodes can belong to more than one management domain.

management LAN A LAN dedicated to the communications necessary for managing systems. It is typically a moderate bandwidth (10/100 baseT) and secured through limited access.

master role A default role that has access to all tools. All tools are automatically associated with the master role, and the master role cannot be deleted from SCM.

multiple-system aware MSA

A run type that supports multi-node operations. Tools with this run type operate on the target nodes using their own internal mechanisms instead of using the distributed task facility. The MSA run type uses the distributed task facility to launch the tool on a single node prior to the tool interacting with the other managed nodes.

MySQL An open source relational SQL database software that is used by SCM for the repository.

node Any device on the network that can communicate with SCM including servers, printers, workstations, hubs, and routers. Nodes must be added to an SCM management domain, and they can be assigned to one or more node groups by a trusted user.

node group A group of nodes defined by a trusted user to divide a network into manageable units. Nodes in a node group usually have something in common like OS type, backup schedule, application type, or hardware type.

repository The database that stores vital information about the managed cluster including: users, nodes, node groups, roles, tools, and authorizations.

role A definition of responsibilities related to an operation or process. Each SCM role is associated with a set of tools.

role-based management A system that uses roles to limit the tools users can access.

Secure Sockets Layer protocol SSL

A security protocol that encrypts and authenticates transactions between the client and the server. It is application protocol independent.

Simple Network Management Protocol SNMP

A protocol of the Internet reference model used for network management.

single-system aware SSA

A run type that doesn't support multi-node operations. Tools with this run type are only aware of the node they are running on.

spoofing A Web site posing as another site to gather confidential or sensitive information, alter data transactions, or present false or misleading data.

standard output STDOUT

The default place to which a program writes its output. The default is the terminal display.

standard error STDERR

The default place where the system writes error messages. The default is the terminal display.

task An executed instance an SCM tool, on one or more nodes or node groups, with a specific set of arguments.

Tomcat An open source implementation of Java Servlet and JavaServer Pages technologies that is used by SCM as a Web server.

tool An application, command, or script that can be executed by SCM on one or more nodes to perform a task.

tool category An organizational structure for grouping tools. A tool must belong to one and only one category. Tool categories can only contain tools; they cannot contain other tool categories.

trusted user A privilege given to one or more users. Trusted users administer the SCM software to enable other users to manage network resources.

user A network user with a valid login on the CMS that has been added to SCM.

WBEM Services HP WBEM Services for HP-UX - A Hewlett-Packard product that uses WBEM and DMTF standards to manage HP-UX system resources.

Web-Based Enterprise Management WBEM

An initiative based on a set of management and Internet standard technologies developed to unify the management of enterprise computing environments.

Web-launch aware WLA

A run type for tools that are launched in a Web browser using a Web server. WLA tools can be designed to deal with multiple systems.

workspace The section of the graphical user interface where tools display.

X client An application or tool that displays on an X server. X clients can also called X applications.

X server A local application that accepts X client requests and acts upon them.

X Window System A cross-platform windowing system that uses the client/server model to distribute services across a network. It enables applications or tools to run on a remote computer.

XML *See extensible markup language*

XML document A collection of data represented in XML.

A

- access, 49
- administering SCM
 - get started, 52
- anonymous ports, 22
 - calculate CMS requirements, 22
 - set socket number range, 23
- audit log, 8, 18, 48
 - configuration, 18
 - configure, 53
 - maintain, 53
 - view, 51
- authorizations, 13, 14
 - add, 53

B

- browser
 - supported versions, 29

C

- CA-signed certificates, 56, 57
- central management server, 10, 11
 - HP-UX install, 30
 - Linux install, 33
 - ports, 21
 - requirements, 28
- certificate authority, 19, 56
- certificate server, 58
- client
 - see network client
- cluster
 - see management domain
- CMS
 - see central management server
- command line interface, 48
- command line tools, 16
- convert tools, 43
- custom scripts and commands, 9
- custom tools, 48

D

- database, 18
- DBAdminPassword, 62
- distributed talk facility, 16
- Distributed Task Facility
 - security, 20
 - see also management protocols
- download software, 26
- DTF
 - see Distributed Task Facility

F

- firewall, 21
- ftp, 19

G

- generated passwords, 62
- getting started
 - administer SCM, 52

- use SCM, 49
- graphical user interface, 48

H

- HP-UX
 - install, 30
 - supported versions for CMS, 28
 - supported versions for managed nodes, 29
- HTTPS, 20

I

- increased security, 23
- information storage, 18
- Insight Manager, 9
- install, 26
 - download software, 26
 - HP-UX CMS, 30
 - Linux CMS, 33
 - managed nodes, 37
 - process, 26
 - system requirements, 28
 - time required, 27
- Internet Explorer
 - supported version, 29
- IPSec, 60

J

- Java keytool, 56, 57
- Java RMI, 20
 - encrypting transactions, 60

K

- keytool, 56, 57

L

- Linux
 - install, 33
 - SNMP requirement, 37
 - supported versions for CMS, 28
 - supported versions for managed nodes, 29
- log on, 49

M

- managed cluster
 - see management domain
- managed nodes, 10
 - install, 37
 - ports, 22
 - requirements, 29
- management domain, 10
- management home page, 51
- management protocols, 10, 16
 - DTF, 16
 - SNMP, 16
 - WBEM, 16
- management tools, 9
- master role, 13, 62
 - CMS caution, 14

Index

Mozilla
 supported version, 29
multi-system management, 8
MxConfigPassword, 62
MxDBUserPassword, 62
MxKeystorePassword, 56, 57, 58, 62
MySQL, 11, 18

N

navigating SCM, 51
Netscape
 supported version, 29
Netscape Directory Server, 43
network client, 12, 48
 requirements, 29
node groups, 10
 add, 53
 delete, 53
nodes, 10
 add, 53
 delete, 53
 select, 49
 view properties, 51
nodes list
 customize, 51

O

operating systems
 supported versions, 28, 29

P

password
 DBAdminPassword, 62
 generated at install, 62
 MxConfigPassword, 62
 MxDBUserPassword, 62
 MxKeystorePassword, 62
 security, 62
patches, 28
ports, 21
 anonymous, 22
 CMS, 21
 configuring, 21
 managed node, 22
protocols, 10
 see also management protocols
 SSL, 19

R

repository, 11, 18
 maintain, 53
requirements
 central management server, 28
 managed node, 29
 network client, 29
 patches, 28
 software on the CMS, 28
 upgrade from 2.5, 41
rlogin, 19

role-based management, 8, 48
roles, 13
 add, 53
 delete, 53
 maximum number of, 13
root permissions, 13

S

SCM
 access, 19
 multiple versions, 41
 navigate, 51
 overview, 8
 restart, 58, 59
 upgrade from 2.5, 41
SecSH, 19
secure
 access, 19
 transactions, 20
secure access encryption, 19
security, 9
 audit log, 62
 authorizations, 62
 firewall, 21
 increased security options, 55
 IPSec, 60
 Java RMI, 60
 network dependencies, 63
 options, 23
 overview, 19
 passwords, 62
 root access, 62
 secure shell, 19
 self-signed certificates, 20
 software dependencies, 63
 Tomcat, 56
 WBEM, 57
 Web server, 61
security management, 63
Security Patch Check, 63
self-signed certificates, 20, 56, 57
SNMP
 community names and passwords, 21
 configuration, 37
 GetRequest, 21
 security, 21
 SetRequest, 21
software
 access, 26
 download, 26
stderr, 18
stdout, 18
system requirements
 central management server, 28
 managed node, 29
 network client, 29

T

tasks, 51

TDEF file
 see XML tool definition file

telnet, 19

Tomcat, 56

 restart, 58, 59

 security, 20

tools, 16, 43

 add, 52, 53

 command line tools, 16

 default authorizations, 13

 delete, 53

 execute, 49, 52

 types, 16

 Web tools, 16

 X Window tools, 16

trusted user, 14, 48, 52, 62

U

update, 45

upgrade, 41

 additional clean-up tasks, 43

 agent compatibility, 41

 manually convert tools, 43

 remove Netscape Directory Server, 43

 requirements, 41

user interfaces, 8, 48

users, 13

 add, 53

 delete, 53

 types of, 48

uses for SCM, 48

 administer the software, 48

 manage network resources, 48

using SCM

 get started, 49

V

version 3.00.04, 45

W

WBEM

 certificate validation, 57

 restart, 58

 security, 20

Web browser, 19

 download, 29

web browser

 supported versions, 29

Web server, 19, 20

 disable, 61

 restart, 61

Web tools, 16

X

X server, 20

X Windows tools, 16

XML tool definition file, 18, 53